Spectral Moment of Order Four and the Uniqueness of the CCZ class of Dublin APN Permutation

Valérie Gillot Philippe Langevin Abdoulaye Lo

Institut de Mathématiques de Toulon, Université de Toulon

Xth Boolean Function and their Application:
Larnaca, Cyprus
September 1-5, 2025

Almost Perfect Nonlinear maps

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$, for $u, v \in \mathbb{F}_2^m$,

$$N(u,v) = \text{number of solutions of } \begin{cases} x + y = u, \\ F(x) + F(y) = v. \end{cases}$$

$$\delta(F) = \max\{N(u,v) : u \neq 0,\ v \in \mathbb{F}_2^m\} \geqslant 2.$$

APN

F is APN $\iff \delta(F) = 2$

cube

x^3 is APN and it is a permutation iff the dimension m is odd

remember good news from Ireland at F_{q^9} !

John Dillon Waterville, Kerry the week before Fq9. . . Kim Browning, Mike Macquistan, Adam Wolfe.

The Big APN Problem

- **2006** — *Xiang-Dong Hou* no APN permutation in dimension 4.
- **2009** — *Dillon and al.* Dublin APN-permutation in 6 variables.

open problem

Existence of APN permutation in **even** dimension greater than 6 ?

open question

Do we know all APN in dimension **6** ?

CCZ-equivalence

Graph of $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$

$$\Gamma(F) = \{(x, F(x)) \mid x \in \mathbb{F}_2^m\} \subseteq \mathbb{F}_2^m \times \mathbb{F}_2^n$$

$$F \underset{\text{CCZ}}{\sim} G \quad \Leftrightarrow \quad \exists\, \mathfrak{T} \in \mathrm{AGL}(m+n), \quad \mathfrak{T}\big(\Gamma(F)\big) = \Gamma(G)$$

Remark

If F is a permutation then $F \underset{\text{CCZ}}{\sim} F^{-1}$

Compatibility

If F is APN and $F \underset{\text{CCZ}}{\sim} G$, then G is APN

EA-equivalence

Two (m, n)-vectorial functions F and G are EA-equivalent if

$$G = A \circ F \circ B + C$$

for some $A \in \mathrm{AGL}(n)$, $B \in \mathrm{AGL}(m)$, and $C \in \mathrm{Aff}(m, n)$.

EA is finer than CCZ

$$F \underset{\text{EA}}{\sim} G \Longrightarrow F \underset{\text{CCZ}}{\sim} G$$

$$\deg_{\min}(F) := \min_{F \underset{\text{CCZ}}{\sim} G} \deg(G) \quad \deg_{\max}(F) := \max_{F \underset{\text{CCZ}}{\sim} G} \deg(G)$$

Known APN classes in 6 variables

14 CCZ classes of APN splitting in **716 EA classes**

all but one have a quadratic representative, all have maximal degree 4.

14 CCZ class of known APN														
# **EA**	25	19	91	19	3	13	91	3	92	85	85	91	13	86

— *minimal degree 3*

— *class of Dublin permutation*

open question

Is there another CCZ class in 6 variables ?

What did one observed ?

- no APN of degree 6 is known
- no APN of degree 5 is known
- most of APN have degree 4
- all APN of degree 3 are known

$$\sharp\text{quartics} = 2^{90} \times \sharp\text{cubics}$$

open question

is there an APN CCZ class purely quartic i.e. minimal degree 4 ?

spectral moment of order 4

Let f be a Boolean function

$$f : \mathbb{F}_2^m \to \mathbb{F}_2$$

Walsh coefficient :

$$\forall a \in \mathbb{F}_2^m, \quad \hat{f}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+a\cdot x}.$$

normalized spectral moment of order 4 (kurtosis) :

$$\kappa(f) = \frac{1}{q^3} \sum_{a \in \mathbb{F}_2^m} \hat{f}(a)^4, \quad q = 2^m.$$

spectral caracterisation

F is APN iff

$$\sum_{0 \neq f \in \langle F \rangle} \kappa(f) = 2(q-1).$$

degree	2	3	4	5	6
♯class	1	3	62	335	686
cumul.	1	4	66	401	1087

number of class of 6-bit Boolean functions with $\kappa(f) \leq 2$

spectral level

Let F be an (m, n)-map.

$$F = (f_1, f_2, \ldots, f_n)$$

component spaces of F :

$$\langle F \rangle := \mathrm{span}(f_1, f_2, \ldots, f_n)$$

spectral set of F :

$$\mathfrak{K}(F) := \{\kappa(f) \mid 0 \neq f \in \langle F \rangle\}$$

The cardinality of $\mathfrak{K}(F)$ is the spectral level of F.

2-spectral level

If the dimension m is even then $\kappa(f) \neq 2$

The spectral level of a 6-bit APN map satisfies $\sharp\mathfrak{K}(F) \geq 2$

A vectorial APN-function F has *2-spectral levels* of type (α, β) when

$$\sharp\mathfrak{K}(F) = \{\alpha, \beta\}, \quad \alpha < \beta.$$

$$\alpha A + \beta B = 2(q-1), \quad A + B = q - 1;$$

$$A := \sharp\{f \in \langle F \rangle \mid \kappa(f) = \alpha\} \qquad B := \sharp\{f \in \langle F \rangle \mid \kappa(f) = \beta\}$$

most of quadratic APN have type (1,4).

One can prove that a 6-bit APN of type (1,4) is quadratic !

Analysis of Dublin permutation

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

Table – Permutation of Dublin has type $(1.75, 4)$

Observation

- 2 spectral levels, $\alpha = 1.75$ (56 comp) and $\beta = 4$ (7 comp),
- 7 components in a 3-dimensional subspace.

In fact the Boolean components splits in exactely two EA-class !

Numerical exploration

In dimension 6, backtracking approachs are sufficientely effective to construct APN-extensions of a given (6,4)-vectorial mapping.

1. 2-switching of known APN — done
2. extension of $(6, 3)$-bent — bent project
3. spectral moment of order 4 — ab-apn project

methods that generate large sets of $(6, 4)$-vectorial mappings that are candidates for APN-extension.

- invariant in (1)+(2)+(3)
- APN-extentibility test (2)+(3)

2-flat condition

Given a vectorial (m, n)-maps G, we define the set of 2-flats :

$$\mathfrak{F}_G := \left\{\text{2-flat } \{x, y, z, t\} \mid G(x) + G(y) + G(z) + G(t) = 0\right\}$$

$$x + y + z + t = 0$$

$$F \text{ is APN} \qquad \Longleftrightarrow \qquad \mathfrak{F}_F = \emptyset \ .$$

The extension $F := (G, g)$ of $G \in \mathrm{Vect}(m, m-2)$ by $g \in \mathrm{Vect}(m, 2)$ is APN iff :

$$\forall \{x, y, z, t\} \in \mathfrak{F}_G \qquad g(x) + g(y) + g(z) + g(t) \neq 0.$$

Looking g as a mapping into the field $\mathbb{F}_4$:

$$g(x) + g(y) + g(z) + g(t) \neq 0 \Leftrightarrow \big(g(x) + g(y) + g(z) + g(t)\big)^3 = 1$$

APN extension test

Looking g as a mapping into the field $\mathbb{F}_4$:

$$g(x)+g(y)+g(z)+g(t)\neq 0 \Leftrightarrow \big(g(x)+g(y)+g(z)+g(t)\big)^3=1$$

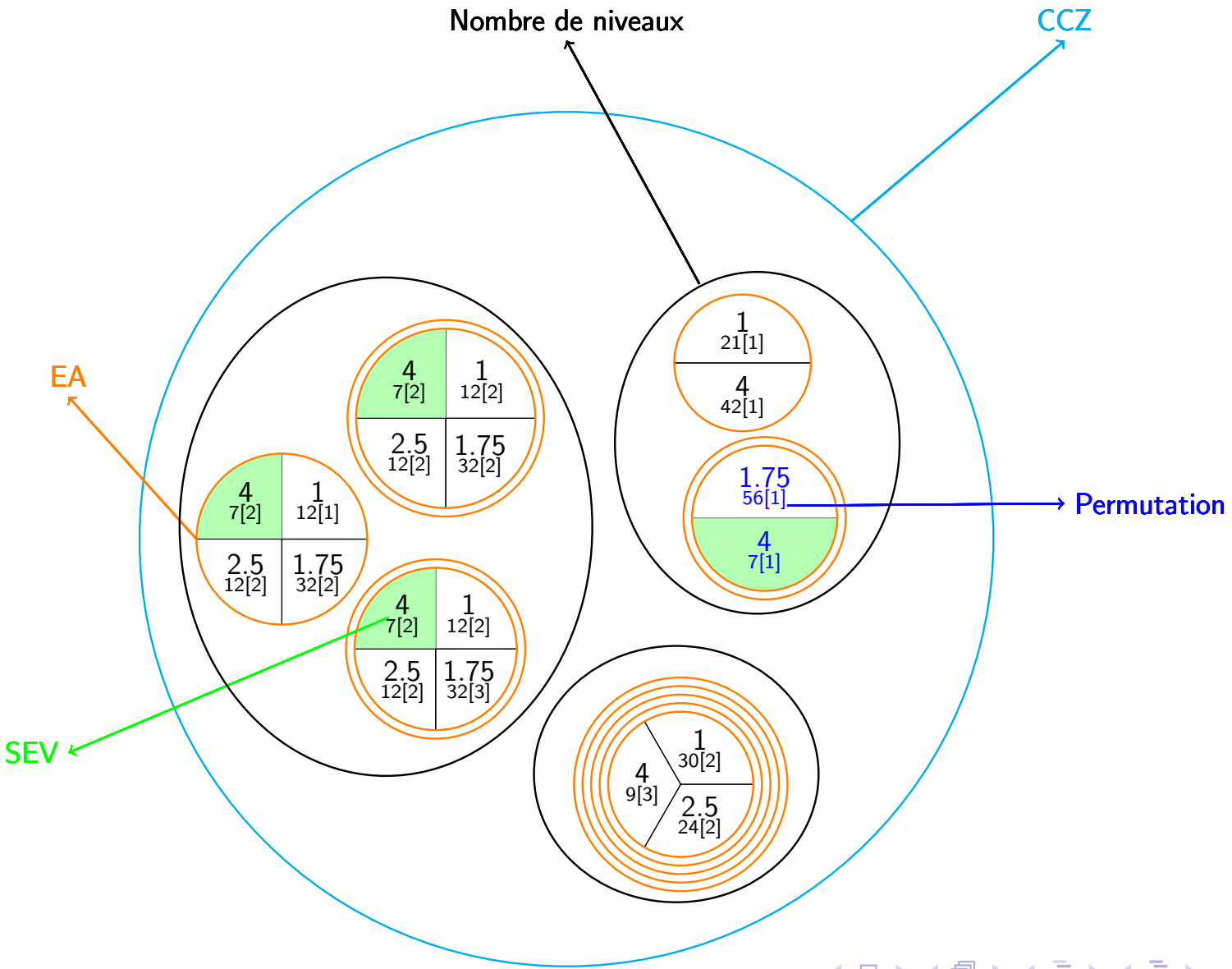
We indroduce in $q(q+1)/2 := q+q(q-1)/2$ *boolean variables* :

$$[x] := g(x)^3, \quad [x,y] := g(x)g(y)\big(g(x)+g(y)\big)$$

$$[x]+[y]+[z]+[t]+[x,y]+[x,z]+[x,t]+[y,z]+[y,t]+[z,t]=1.$$

no solution $\Longrightarrow$ not APN-extendable !

Dissection of CCZ-class of Dublin



challenge

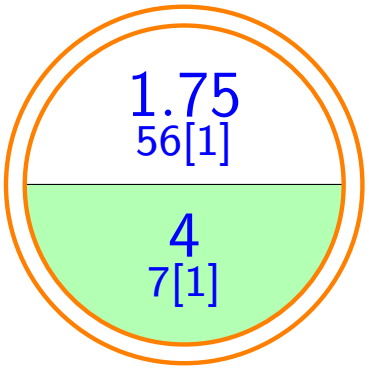
What are the CCZ-classes sharing the same shape that Dublin permutation ?

$$\mathfrak{K}(F) = \{1.75, 4\}$$

and $\langle F \rangle$ contains

- 3-dimensional space of cubics with $\kappa = 4.0$
- 56 quartics with $\kappa = 1.75$

Method of attack



- enumerate all $(6, 4)$-quartic satisfying (*)
- keep the maps that are APN-expandable
- find APN-expansion by backtraking
- extract 2-spectral level function
- compare with Dublin permutation

(*) 8 quartics $\kappa = 1.75$, 7 cubics $\kappa = 4.0$.

key points

The procedure depends EA-invariant algorithm !

- Only eight EA-classes of quartics with $\kappa = 1.75$
- A fast algorithm to check APN-expandibility
- 1 week of computation using 72 cores

At the end :

Uniqueness of the CCZ class of Dublin Permutation

other pairs involving spaces ?

α	A	degree	classe	β	B	degree	classe
1.0000	(56)	23...	4	10.0000	(7)	.3...	1
1.0000	(15)	23...	4	2.3125	(48)	.34..	214
1.0000	(7)	23...	4	2.1250	(56)	..4..	49
1.7500	(56)	..4..	8	4.0000	(7)	234..	86
1.9375	(56)	..4..	54	2.5000	(7)	.34..	216
1.9375	(62)	..4..	54	5.8750	(1)	..4..	19

ab-APN project

α	A	deg	♯	β	B	deg	♯
1.0	42	23.	4	4.0	21	234	86
1.0	60	23.	4	22.0	3	.3.	1
1.0	56	23.	4	10.0	7	.3.	1
1.0	49	23.	4	5.50	14	.34	29
1.0	21	23.	4	2.50	42	.34	216
1.0	57	23.	4	11.50	6	.34	5
1.0	35	23.	4	3.250	28	.34	191
1.0	15	23.	4	2.3125	48	.34	214
1.0	51	23.	4	6.250	12	..4	13
1.0	47	23.	4	4.9375	16	..4	37
1.0	39	23.	4	3.6250	24	..4	67
1.0	7	23.	4	2.1250	56	..4	49
1.0	55	23.	4	8.8750	8	..4	2

α	A	deg	♯	β	B	deg	♯
1.750	56	..4	8	4.0	7	234	86
1.750	42	..4	8	2.50	21	.34	216
1.750	60	..4	8	7.0	3	.34	3
1.750	51	..4	8	3.0625	12	.34	321
1.750	35	..4	8	2.3125	28	.34	214
1.750	59	..4	8	5.6875	4	..4	25
1.750	21	..4	8	2.1250	42	..4	49
1.750	49	..4	8	2.8750	14	..4	119
1.750	57	..4	8	4.3750	6	..4	34
1.9375	56	..4	54	2.50	7	.34	216
1.9375	60	..4	54	3.250	3	.34	191
1.9375	42	..4	54	2.1250	21	..4	49
1.9375	62	..4	54	5.8750	1	..4	19

26 possibles type (α, β) for 2 level APN-quartic.

conclusion

We have accumulated numerical evidences that seems to prove that all 6-bit APN-functions are known. However, we are still far from being able to produce numerical/theorical proof without further progress.

find a way to finish bent project and ab-APN project with and without space conditions

1. test for APN-extendibility of $(6, 3)$-maps ?
2. maximal degree of an APN ?
3. algorithmic criterion to eliminate bad compoents ?

rush

In dimension 6, if F has type $(1, 4)$ then F is quadratic.